Title (en)
KEY NEGOTIATION METHOD AND APPARATUS

Title (de)
VERFAHREN UND VORRICHTUNG ZUR SCHLÜSSELVERHANDLUNG

Title (fr)
APPAREIL ET PROCÉDÉ DE NÉGOCIATION DE CLÉ

Publication
EP 3499834 A1 20190619 (EN)

Application
EP 16916069 A 20160919

Priority
CN 2016099366 W 20160919

Abstract (en)
Embodiments of the present invention provide a key negotiation method and apparatus. The method includes: obtaining, by a first base station, a selected key generation capability, and generating a first key parameter based on the selected key generation capability; sending, by the first base station, the first key parameter to a second base station, where the first key parameter is forwarded by the second base station to a terminal; and obtaining, by the first base station, a second key parameter generated by the terminal, and generating a first base key based on the first key parameter and the second key parameter. The first base station independently generates the base key, and the second base station plays only a role of parameter transfer. In this way, it can be ensured that the second base station cannot learn of the base key generated by the first base station, thereby ensuring key security.

IPC 8 full level
H04L 29/06 (2006.01); H04W 12/04 (2009.01); H04L 9/08 (2006.01); H04W 76/15 (2018.01)

CPC (source: EP KR US)
H04L 9/0819 (2013.01 - KR); H04L 9/0877 (2013.01 - US); H04L 63/205 (2013.01 - EP KR US); H04W 12/04 (2013.01 - EP US);
H04W 12/041 (2021.01 - EP KR US); H04W 12/0433 (2021.01 - US); H04W 12/0471 (2021.01 - EP KR US); H04W 76/15 (2018.01 - KR);
H04L 9/08 (2013.01 - EP US); H04W 76/15 (2018.01 - EP US)

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)
BA ME

DOCDB simple family (publication)
EP 3499834 A1 20190619; EP 3499834 A4 20190619; EP 3499834 B1 20211201; BR 112019004840 A2 20190604; CN 109417470 A 20190301;
CN 109417470 B 20211015; KR 20190045287 A 20190502; US 2019208416 A1 20190704; WO 2018049689 A1 20180322

DOCDB simple family (application)
EP 16916069 A 20160919; BR 112019004840 A 20160919; CN 2016099366 W 20160919; CN 201680087551 A 20160919;
KR 20197009436 A 20160919; US 201916298387 A 20190311